

1 ERIK S. SYVERSON (BAR NO. 221933)
esyverson@raineslaw.com
2 RAINES FELDMAN LLP
1800 Avenue of the Stars, 12th Floor
3 Los Angeles, California 90067
Telephone: (310) 440-4100
4 Facsimile: (310) 765-7730

5 Attorneys for Plaintiff Carson Block

6
7 **UNITED STATES DISTRICT COURT**
8 **NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION**
9

10 CARSON BLOCK, an individual ;

11 Plaintiff,

12 v.

13 EQUIFAX, INC., a Georgia Corporation;
14 RICHARD F. SMITH, an Individual,
SUSAN MAULDIN, an Individual,
15 MARY HANNAN, an Individual,
GRAEME PAYNE, an Individual,
16 HAROLD BOUTIN, an Individual,
ROBERT FRIEDRICH, an Individual,
17 VIDYA SAGAR JAGADAM, an
Individual, LARA PEARSON, an
18 Individual, SHEA GIESLER, an
Individual, CLIFF BARBIER, an
19 Individual, JOE SANDERS, an
Individual, and DOES 1 through 25,
20 inclusive;

21 Defendants.

Case No. 17-5367

COMPLAINT FOR:

(1) Negligence; and
(2) Violations of Unfair Competition
Law (Cal. Bus. & Prof. Code § 17200,
***et seq.*)**

DEMAND FOR JURY TRIAL

1 Plaintiff Carson Block (“Block” or “Plaintiff”) files this Complaint against
2 Equifax, Inc. (“Equifax” or “the Company”), and responsible officers, employees,
3 and agents thereof, including Richard F. Smith, the Chairman of the Board and
4 Chief Executive Officer of Equifax, Susan Mauldin, the Chief Information Security
5 Officer (CISO) at Equifax, Mary Hannan, the Senior Vice President, Corporate
6 Technology Legal and Security Support at Equifax, Graeme Payne, the Vice
7 President of IT Risk and Compliance at Equifax, Harold Boutin, the Senior Vice
8 President - IT Strategy and Effectiveness at Equifax, Robert Friedrich, the SVP/CIO
9 Global Consumer Solutions at Equifax, Vidya Sagar Jagadam, the Vice President,
10 IT Governance, Risk & Compliance at Equifax, Lara Pearson, the Senior Director of
11 Risk Security Programs at Equifax, Shea Giesler, the Vice President, Security
12 Programs at Equifax, Cliff Barbier, the Director, Security Engineering Solutions at
13 Equifax, Joe Sanders, an individual of residence unknown, was the Senior Director
14 of Security Engineering Solutions at Equifax, and DOES 1 through 25, inclusive,
15 and alleges the following based on personal knowledge, the investigation of counsel,
16 and information and belief:

17 **I. INTRODUCTION**

18 1. Equifax is in the business of selling consumer credit and insurance
19 reports and related analytics to businesses in a range of industries. As one of the
20 three major credit reporting companies in the United States that collects and
21 aggregates financially sensitive personally identifiable information (“PII”), Equifax
22 is regularly entrusted with the storage, and security of PII. Equifax stores PII
23 relating to over 800 million individual consumers and more than 88 million
24 businesses worldwide. In the United States, the PII held by Equifax includes names,
25 Social Security numbers, birth dates, driver’s license numbers, and credit card
26 numbers.

27 2. According to Equifax, on July 29, 2017, it discovered that “criminals
28 exploited a U.S. website application vulnerability” (“the Vulnerability”) in its

1 system to “gain access to certain files” “potentially impacting information relating
2 to approximately 143 million U.S. consumers.” (the “Data Breach”). The
3 information accessed by the “criminals” “primarily includes names, Social Security
4 numbers, birth dates, addresses and, in some instances, driver's license numbers,”
5 along with credit card numbers and dispute documents with other PII for a smaller
6 subset of consumers.

7 3. In the period shortly after the discovery of the Data Breach, on July 29,
8 2017, and well before the public disclosure of the breach, Equifax managers sold
9 shares worth almost \$1.8 million.

10 4. It was not until 40 days after the Data Breach was discovered that
11 Equifax finally made a limited public disclosure, admitting the scope of the breach
12 via a press release and notifications to the Attorneys General of California and other
13 States. Equifax decided to mail notices to the small percentage of consumers
14 believed to have been affected by the credit card or dispute document disclosures,
15 but not the 143 million or more that had their other PII had exposed to criminals.
16 Instead, for those consumers, Equifax expected consumers to check for themselves
17 on a poorly designed, unreliable, and potentially insecure website,
18 www.equifaxsecurity2017.com.

19 5. As a result of the Data Breach, Block has suffered injuries stemming
20 from an immediate and heightened risk of all manners of identity theft, including but
21 not limited to:

- 22 a. Theft of their personal and financial information;
- 23 b. Costs associated with the detection and prevention of identity
24 theft and unauthorized use of personal information and/or financial
25 accounts;
- 26 c. Unauthorized debit and/or credit account charges;
- 27 d. Loss of use of and/or access to account funds and costs
28 associated with inability to obtain money from accounts or being

1 limited in the amount of money they were permitted to obtain from
2 their accounts, including consequential damages such as missed
3 payments on bills and loans, late charges and fees, and adverse effects
4 on their credit including decreased credit scores and adverse credit
5 notations;

6 e. Costs associated with time spent and the loss of productivity
7 from taking time to address and attempt to ameliorate, mitigate and
8 deal with the actual and future consequences of the data breach,
9 including finding fraudulent charges, cancelling and reissuing cards,
10 purchasing credit monitoring and identity theft protection services,
11 imposition of withdrawal and purchase limits on compromised
12 accounts, and the stress, nuisance and annoyance of dealing with all
13 issues resulting from the Equifax data breach;

14 f. The imminent and certainly impending injury flowing from
15 potential fraud and identify theft posed by their credit card and personal
16 information being placed in the hands of criminals and already misused
17 via the sale of Plaintiffs' and Class members' information on the
18 Internet and/or black market; and

19 g. Damages to and diminution in value of personal and financial
20 information held and exposed by Equifax.

21 6. Equifax was negligent in taking the necessary precautions required to
22 safeguard and protect Plaintiff's PII from criminals, and also breached its duty to
23 timely and adequately disclose the Data Breach.

24 7. Furthermore, Equifax is in violation of the Unfair Competition Law,
25 Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL") for failing to take reasonable
26 measures in protecting Plaintiff's PII

27 **II. THE PARTIES**

28 8. Plaintiff Carson Block is an individual consumer and resident of San

1 Francisco County, California. On or about September 8, 2017, Block entered his
2 information on equifaxsecurity2017.com and subsequently received a message from
3 Equifax informing him that his PII had been stolen by cybercriminals in the Data
4 Breach. As a result of the Data Breach Plaintiff has suffered a loss of privacy, is at a
5 continuous high risk of identity theft or other types of financial fraud, and will
6 continue to suffer from the increased financial and mental costs necessary to
7 consistently monitor and guard against the aforementioned risks.

8 9. Equifax Inc. is a multi-billion dollar corporation, incorporated in
9 Georgia, and headquartered in Atlanta, Georgia. Equifax operates through various
10 subsidiaries including Equifax Information Services, LLC, and Equifax Consumer
11 Services, LLC aka Equifax Personal Solutions aka PSOL. Each of these entities
12 acted as agents of Equifax or in the alternative, acted in concert with Equifax as
13 alleged in this complaint.

14 10. On information and belief, Richard F. Smith, an individual of residence
15 unknown, was the Chairman of the Board and Chief Executive Officer of Equifax at
16 the time of the Data Breach, where had had the responsibility for the operations of
17 Equifax and failed to use his authority to strengthen Equifax's defenses against
18 cybercrimes such as the Data Breach.

19 11. On information and belief, Susan Mauldin, an individual of residence
20 unknown, was the Chief Information Security Officer (CISO) at Equifax at the time
21 of the Data Breach. On information and belief, the CISO of Equifax was directly
22 responsible for management of Equifax's employees or officers maintaining the
23 confidentiality, availability, and integrity of Equifax's consumer data and the
24 security of the assets of the company, such as the PII subject to the Data Breach.

25 12. On information and belief, Mary Hannan, an individual of residence
26 unknown, was the Senior Vice President, Corporate Technology Legal and Security
27 Support at Equifax at the time of the Data Breach. On information and belief, in this
28 role at Equifax Ms. Hannan was the strategic leader responsible for IT tools support

1 and compliance in connection with legal and security business units and for
2 oversight of hardware/software asset management.

3 13. On information and belief, Graeme Payne, an individual of residence
4 unknown, was the Vice President of IT Risk and Compliance at Equifax at the time
5 of the Data Breach. On information and belief, in this role at Equifax Mr. Payne
6 was Responsible for leading initiatives around IT risk and compliance, including
7 access management, IT risks and controls, regulatory compliance, asset
8 management, software compliance and contracts

9 14. On information and belief, Harold Boutin, an individual of residence
10 unknown, was the Senior Vice President - IT Strategy and Effectiveness at Equifax
11 at the time of the Data Breach. On information and belief, in this role at Equifax
12 Mr. Payne was responsible for delivery of the IT Business Strategic plan, including
13 IT Risk Governance to manage all risks related to Technology. This includes
14 Access Management, deliverables required for Internal and External auditors, Asset
15 Management, Software compliance, Software license agreement and IT Financial
16 risks.

17 15. On information and belief, Robert Friedrich, an individual of residence
18 unknown, was the SVP/CIO Global Consumer Solutions at Equifax at the time of
19 the Data Breach. On information and belief, in this role at Equifax Mr. Friedrich
20 was responsible for developing and maintaining Consumer facing platforms and
21 applications for Equifax in the US, UK, and Canada, including platforms for
22 eCommerce and Mobile products.

23 16. On information and belief, Vidya Sagar Jagadam, an individual of
24 residence unknown, was the Vice President, IT Governance, Risk & Compliance at
25 Equifax at the time of the Data Breach. On information and belief, in this role at
26 Equifax Mr. Jagadam's was responsible for IT Governance, Risk Management, IT
27 Compliance with Security and Regulatory requirements, Identity & Access
28 Management, PCI program, IT Controls and Compliance.

1 17. On information and belief, Lara Pearson, an individual of residence
2 unknown, was the Senior Director of Risk Security Programs at Equifax at the time
3 of the Data Breach. On information and belief, in this role at Equifax Ms. Pearson
4 was responsible for Information Security Risk and Compliance and leading highly
5 visible information security programs and was experienced in Information Security
6 Policy & Standard Development.

7 18. On information and belief, Shea Giesler, an individual of residence
8 unknown, was the Vice President, Security Programs at Equifax at the time of the
9 Data Breach. On information and belief, in this role at Equifax Mr. Giesler was
10 responsible for global strategy for ISO 27001 (information security management
11 system standard) compliance, national strategy for FISMA compliance,
12 development of all company security policies, development of security metrics
13 reportable to the CSO, and the security exception process and first level review
14 team.

15 19. On information and belief, Cliff Barbier, an individual of residence
16 unknown, was the Director, Security Engineering Solutions at Equifax at the time of
17 the Data Breach. On information and belief, in this role at Equifax Mr. Barbier was
18 responsible for information security issues and proper governance, risk
19 management, & compliance.

20 20. On information and belief, Joe Sanders, an individual of residence
21 unknown, was the Senior Director of Security Engineering Solutions at Equifax at
22 the time of the Data Breach. On information and belief, in this role at Equifax Mr.
23 Sanders was responsible for Application Security and Vulnerability Management
24 Global Leader, Data Loss Prevention, Application Security, and Vulnerability
25 Management, Monitoring and responding to intrusion prevention systems alerts.

26 21. Plaintiff does not know the true names or capacities, whether
27 individual, associate, corporate, or otherwise, of the defendants sued herein as
28 DOES 1 through 25, inclusive, and Plaintiff therefore sue said defendants by such

1 fictitious names. Plaintiff will amend this Complaint to state the true names and
2 capacities of these defendants once Plaintiff discovers this information. Plaintiff is
3 informed and believes, and based thereon alleges, that like Mauldin, Hannan, Payne,
4 Boutin, Friedrich, Jagadam, Pearson, Giesler, Barbier, Sanders, each of the DOE
5 Defendants sued herein by a fictitious name is in some way liable and responsible to
6 Plaintiff on the facts herein alleged for Plaintiff's damages in connection with the
7 Data Breach and the negligent operations of Equifax, either as employees or officers
8 of Equifax responsible for ensuring that massive security lapses that led to the Data
9 Breach or negligent reporting that followed its discovery did not occur, or as
10 contractors, subsidiaries, or others to whom Equifax and its officers and employees
11 delegated such authority. Equifax, Smith, Mauldin, Hannan, Payne, Boutin,
12 Friedrich, Jagadam, Pearson, Giesler, Barbier, Sanders, and DOES 1 through 25,
13 inclusive shall be referred to collectively as "Defendants."

14 **III. JURISDICTION AND VENUE.**

15 22. This Court has jurisdiction pursuant to 28 U.S.C. § 1332 because there
16 is complete diversity of citizenship between Plaintiff and Defendants, and the
17 amount in controversy exceeds \$75,000, exclusive of interest and costs.

18 23. This Court has personal jurisdiction over Equifax because Equifax
19 maintains offices in California, conducts business in California, and has sufficient
20 minimum contacts with California to satisfy Due Process standards.

21 24. On information and belief, the Court has personal jurisdiction over
22 defendants Mauldin and the Doe Defendants as a result of sufficient minimum
23 contacts with California in connection with the Data Breach and the harm caused
24 thereby to Plaintiff Block.

25 25. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)
26 because a substantial part of the events or omissions giving rise to Plaintiff's claims
27 occurred in this District.

28

1 **IV. FACTUAL BACKGROUND.**

2 **A. EQUIFAX'S BUSINESS OF STOCKPILING PERSONAL**
3 **INFORMATION**

4 26. Equifax was founded in Atlanta, Georgia, as Retail Credit Company in
5 1899. Equifax is one of the three main credit reporting companies in the United
6 States. The Company's business revolves around being a secure storehouse for PII,
7 including financial information, and providing a clear financial profile of consumers
8 that lenders and other businesses can rely on.

9 27. Equifax organizes, assimilates and analyzes data on more than 820
10 million consumers and more than 91 million businesses worldwide, and its database
11 includes employee data contributed from more than 7,100 employers.

12 28. Equifax has seen wide growth as a company based on its use of
13 sensitive financial and personal consumer data. From 2015 to 2016, the company
14 saw operating revenues grow 18% to \$3.14 billion. In 2016, Richard F. Smith, the
15 Chairman of the Board and Chief Executive Officer of Equifax received a total
16 compensation package of \$14,964,600. Despite the impact of the public disclosure
17 of the data breach, Equifax's current market capitalization of over \$14 billion
18 dollars.

19 29. Equifax has collected and/or stored PII regarding Carson Block,
20 including his Social Security number, birth date, home driver's license information,
21 and credit card information.

22 **B. EQUIFAX'S ABYSMAL HANDLING OF A MASSIVE BREACH**
23 **OF ITS STOCKPILE OF CONSUMER PERSONAL**
24 **INFORMATION**

25 30. From about May 2017 through July 2017, Equifax suffered from a self-
26 described "website application vulnerability" which left Block's PII vulnerable to
27 criminals and cyber-attack.
28

1 31. On or about July 29, 2017, Equifax discovered that criminals had
2 exploited the “website application vulnerability” in its system and stolen the PII
3 information of over 143 million individuals.

4 32. Presumably realizing the severe negative this information would have
5 on Equifax’s stock price, three of Equifax insiders made substantial sales of Equifax
6 stock within days of the discovery of the massive Data Breach. On Monday, August
7 1, 2017, Chief Financial Officer John Gamble sold Equifax shares worth \$946,374,
8 approximately 13 percent of his Equifax holdings. On the same day, Joseph
9 Loughran, President of U.S. Information Solutions exercised options to dispose of
10 Equifax stock worth \$584,099, approximately 9 percent of his Equifax holdings. On
11 August 2, 2017, Rodolfo Ploder, President of Workforce Solutions, sold \$250,458 of
12 Equifax stock, almost 4 percent of his holdings.

13 33. Among them, these three Equifax senior executives sold Equifax shares
14 worth almost \$1.8 million in the days following the discovery of the data breach on
15 July 29, 2017, all while Equifax delayed public disclosure of the breach of the
16 millions of innocent victims that their personal information, which had been
17 compromised due to Equifax’s negligence.

18 34. On September 7, 2017, Equifax issued a press release announcing that
19 “[c]riminals exploited a U.S. website application vulnerability to gain access to
20 certain files” in Equifax systems. The breach began in mid-May and continued until
21 it was discovered by Equifax on July 29, 2017. The release stated that “[t]he
22 information accessed primarily include[d] names, Social Security numbers, birth
23 dates, addresses and, in some instances, driver’s license numbers. In addition, credit
24 card numbers for approximately 209,000 U.S. consumers, and certain dispute
25 documents with personal identifying information for approximately 182,000 U.S.
26 consumers, were accessed. As part of its investigation of this application
27 vulnerability, Equifax also identified unauthorized access to limited personal
28

1 information for certain UK and Canadian residents.” The unauthorized access
2 potentially impacted “approximately 143 million U.S. consumers.”

3 35. Upon this disclosure Equifax shares tumbled over 6 percent from
4 around \$142 to around \$125 in after-hours trading.

5 36. Equifax further opted to only notify consumers of the breach via mail if
6 they were among the small percentage whose credit card numbers or dispute
7 documents were accessed. For the remaining millions of consumers, Equifax
8 required them to proactively turn to its poorly designed, unreliable, and potentially
9 insecure website, equifaxsecurity2017.com, where consumers could provide Equifax
10 with personal information to determine whether their data may have been
11 compromised.

12 37. Equifax also “offered” those impacted by the data breach one year of
13 “complimentary” credit monitoring and identity theft protection, but requiring a
14 consumer’s credit card which would be subject to automatic renewal charges if not
15 proactively terminated. Rather than actually attempting to assist the affected
16 consumers, Equifax continued its poor judgment and turned its data breach into a
17 massive marketing opportunity.

18 **C. EQUIFAX’S ONGOING HISTORY OF DATA BREACHES AND**
19 **LACK OF ADEQUATE PRECAUTIONS.**

20 38. Equifax knew or should have known that its system was at-risk for
21 attack based on previous attacks and reports that its internal system had weaknesses.

22 39. Equifax knew of problems with its data security, at least as a result of
23 two substantial data breaches that occurred in 2016 alone. In one, hackers took W-2
24 tax data from an Equifax subsidiary called TALX; the breach (caused by hackers
25 using personal information to guess client customer questions and ultimately reset
26 their 4-digit PIN and gain access to customers’ tax data) went undiscovered from
27 nearly a year. In another, Equifax’s W-2 Express website was breached in May
28 2016 (a result of using alarmingly poor security for the generation of PINs from the

1 last four digits of a SSN and the four digit year of birth) , leading to the leak of
2 430,000 names, addresses, social security numbers, and other information.

3 40. Equifax also suffered a smaller data breaches. One in January 2017
4 concerning LifeLock customer credit information. Another breach of credit reports
5 in 2013-2014 using personal information. In 2016, a vulnerability to cross-site
6 scripting was discovered on Equifax's website, potentially as a result of Equifax
7 using old and discontinued technology. .

8 41. On September 13, 2017, Equifax confirmed that the Data Breach
9 included the exploit of a US website application vulnerability, Apache Struts CVE-
10 2017-5638. This flaw in Apache Struts framework and the fix for it was publicly
11 disclosed on March 6, 2017. Within days, massive attacks based on the
12 vulnerability were already being reported. More than two months later, the Equifax
13 Data Breach occurred, apparently because Equifax failed to apply the publicly
14 available fix to Apache Struts within its US website applications, despite
15 demonstrable proof and public reporting that the vulnerability gave real-world
16 attackers an easy way to take control of sensitive websites.

17 **FIRST CAUSE OF ACTION**

18 **(Negligence- Against All Defendants)**

19 42. Plaintiff re-alleges and incorporates by reference all prior allegations as
20 if fully set forth herein.

21 43. Defendants owed a duty to Plaintiff to exercise reasonable care in
22 obtaining, retaining, securing, safeguarding, deleting, and protecting their personal
23 and financial information in its possession from being compromised, lost stolen,
24 accessed, and misused by unauthorized persons. This duty included, among other
25 things, designing, maintaining, and testing Equifax's security system to ensure that
26 Plaintiffs' and the Class's personal and financial information in Equifax's
27 possession was adequately secured and protected. Defendants further owed a duty
28 to ensure that Equifax's internet security measures were up to date and regularly

1 tested. Defendants further owed a duty to Plaintiff to implement processes that
2 would detect a breach of its security system in a timely manner and to timely act
3 upon warnings and alerts, including those generated by its own security systems.

4 44. Defendants owed a duty to Plaintiffs and the Class to ensure Equifax's
5 security was consistent with industry standards and requirements, to ensure that its
6 computer systems and networks, and the personnel responsible for them, adequately
7 protected the personal and financial information of Plaintiff held by Equifax.

8 45. Defendants knew Equifax solicited, gathered, and stored the personal
9 and financial data of Plaintiffs and the Class to facilitate credit reports and
10 monitoring. Defendants knew Equifax inadequately safeguarded such information
11 on its computer systems and that hackers routinely attempt to access this valuable
12 data without authorization. Defendants had prior notice that Equifax's systems were
13 inadequate by virtue of the earlier breaches that preceded this one and by security
14 updates and bulletins regarding systems used by Equifax, but continued to maintain
15 those inadequate systems to the ultimate detriment of consumers like Plaintiff.
16 Defendants knew or should have known that a breach of Equifax systems would
17 cause damages to Plaintiff and Defendants had a duty to adequately protect such
18 sensitive personal and financial information

19 46. Plaintiff was a foreseeable victim of any inadequate safety and
20 security practices. Plaintiff had no ability to protect the data that was in Equifax's
21 possession from Defendants' negligent security practices, actions, and choices.

22 47. In addition, Defendants had a duty to timely and adequately disclose to
23 Plaintiff that his PII had been compromised. Such timely disclosure was necessary
24 to allow Plaintiff to take appropriate measures to avoid unauthorized charges to
25 credit or debit card accounts, cancel or change usernames and passwords on
26 compromised accounts, monitor account information and credit reports for
27 fraudulent activity, contact banks or other financial institutions that issue his credit
28 or debit cards, obtain credit monitoring services, and take other steps to mitigate or

1 ameliorate the damages caused by Defendants' misconduct.

2 48. Defendants knew, or should have known, the risks inherent in Equifax
3 collecting and storing the personal and financial information of consumers like
4 Plaintiff, and of the critical importance of providing adequate security of that
5 information.

6 49. Defendants breached their duty to Plaintiff by failing to maintain
7 proper security measures, policies and procedures, and training. Defendants failed
8 to timely notify Plaintiff of the Data Breach, waiting over a month from discovery
9 of the hack to publicly announcing the breach while Equifax executives unloaded
10 stock. Plaintiff has been harmed as a direct and proximate result of Defendants'
11 negligence. Plaintiff will continue to be harmed as a direct and proximate result of
12 Defendants' negligence, including but not necessarily limited to: a) out-of-pocket
13 costs associated with addressing false tax returns filed with the IRS and state tax
14 agencies; b) increased future out of pocket costs in connection with preparing and
15 filing tax returns; c) out-of-pocket costs associated with procuring identity
16 protection and restoration services; d) in the event of future identity theft, out-of-
17 pocket costs associated with repairing credit, reversing fraudulent charges, and other
18 harms; and e) lost productivity and enjoyment as a result of time spent monitoring,
19 addressing and correcting future consequences of the Data Breach.

20 50. Holding Defendants accountable for their negligence will further the
21 policies underlying negligence law and will require Defendants and encourage
22 similar persons that work with, obtain and retain sensitive consumer personal and
23 financial information to adopt, maintain and properly implement reasonable,
24 adequate and industry-standard security measures to protect such customer
25 information.

26 51. Plaintiff is entitled to money damages for all out-of-pocket costs caused
27 by Defendants' negligence, and has suffered damages in an amount to be proven at
28 trial.

SECOND CAUSE OF ACTION

(Violation of Unfair Competition Law California Business and Professional

Code Section 17200, *et seq.*- Against Equifax)

52. Plaintiff re-alleges and incorporates by reference all prior allegations as if fully set forth herein.

53. Equifax engaged in unfair and unlawful business practices in violation of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* (“UCL”). Equifax’s acts, omissions, and conduct constitute unfair and unlawful business practices under the UCL.

54. Equifax’s practices were unlawful and in violation of Civil Code section 1798.81.5 of the Customer Records Act (“CRA”) because Equifax failed to take reasonable measures in protecting Plaintiff’s PII.

55. Equifax’s practices were unlawful and in violation of Civil Code section 1798.82 of the CRA because Equifax failed to timely or adequately disclose that Plaintiff’s PII had been breached by hackers.

56. Equifax’s acts, omissions, and conduct also constitute “unfair” business acts or practices because they offend public policy and constitute immoral, unethical, and unscrupulous activities that caused substantial injury, to Plaintiff and others. The gravity of harm resulting from Equifax’s conduct outweighs any potential benefits attributable to the conduct and there were reasonably available alternatives to further Equifax’s legitimate business interests.

57. Equifax has exclusive knowledge about the extent of the Data Breach, including during the days and weeks following the Data Breach.

58. As a direct and proximate result of Equifax’s unlawful and unfair business practices as alleged herein, Plaintiff has suffered injury in fact. Plaintiff has been injured in that his personal and financial PII has been compromised, subject to identity theft, identity fraud, and/or is at risk for future identity theft and fraudulent

1 activity on their financial accounts.

2 59. As a direct and proximate result of Equifax's unlawful and unfair
3 business practices as alleged herein, Plaintiff already suffers from identity theft,
4 identity and financial fraud, and/or a continuing increased risk of identity theft and
5 financial fraud due to the compromise, publication, and/or unauthorized use of his
6 financial PII. Plaintiff has also been injured by, among other things: (1) the loss of
7 the opportunity to control how his PII is used; (2) the compromise, publication,
8 and/or theft of their PII; (3) out-of-pocket costs associated with the prevention,
9 detection, and recovery from identity theft and/or unauthorized use of financial
10 accounts; (4) lost opportunity costs associated with effort expended and the loss of
11 productivity from addressing and attempting to mitigate the actual and future
12 consequences of the breach, including but not limited to efforts spent researching
13 how to prevent, detect, contest and recover from identity fraud; (5) costs associated
14 with the ability to use credit and assets frozen or flagged due to credit misuse,
15 including complete credit denial and/or increased costs to use credit, credit scores,
16 credit reports and assets; (6) unauthorized use of compromised PII to open new
17 financial accounts; (7) tax fraud and/or other unauthorized charges to financial
18 accounts and associated lack of access to funds while proper information is
19 confirmed and corrected; (8) the continued risk to his PII and the PII of family
20 members which remain in Equifax's possession and are subject to further breaches
21 so long as Equifax fails to undertake appropriate and adequate measures to protect
22 the PII in its possession; and (9) future costs in terms of time, effort and money that
23 will be expended to prevent, detect, contest, and repair the impact of the PII
24 compromised as a result of the Data Breach for the remainder of the Plaintiff's life.

25 60. As a result of Equifax's violations of the UCL, Plaintiff is entitled to
26 injunctive relief, including, but not limited to an order preventing Equifax from
27 engaging in the negligent practices that lead to the Data Breach.
28

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment against Defendants as follows:

- A. A finding that Defendant breached their duty to safeguard and protect Plaintiff's PII which was compromised in the Data Breach;
- B. An award of damages against Defendants and in favor of Plaintiff, including actual damages, punitive damages, and/or statutory damages according to proof, but at least \$500,000;
- C. Award equitable, injunctive, and declaratory relief as appropriate;
- D. For attorney fees, costs of suit and prejudgment and post-judgment interest, as provided under applicable law; and
- E. For such other, further, and/or different relief, in law or equity, as the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff hereby demands a trial by jury, including pursuant to Federal Rule of Civil Procedure 38(b), on all issues where a right to such trial exists.

Dated: September 15, 2017

RAINES FELDMAN LLP

By: /s/ Erik S. Syverson
ERIK S. SYVERSON
Attorneys for Plaintiff Carson Block